Claim Amendment Summary

Claims pending

- At time of the Action: Claims 1-49.
- After this Response: Claims 1-49.

Canceled or Withdrawn claims: none.

Amended claims: 14, 23, 34, 42 and 43.

New claims: none.

Please amend claims 14, 23, 34, 42 and 43 as follows:

1. **(ORIGINAL)** An authentication system comprising:

a host network configured to provide access to the Internet from a public location;

at least one authentication component communicatively linked with the host network and configured to enable authentication of individual users so that they can access the Internet through the host network, authentication being configured to take place in a manner that is independent of any user affiliation with any Internet Service Providers (ISPs);

at least one access module communicatively linked with the one authentication component and configured to enable a user to access the host network; and

an authentication database communicatively linked to the host network and containing user information that can be used to authenticate a user.

2. **(ORIGINAL)** The system of claim 1, wherein the authentication database comprises a globally accessible authentication database.

3. **(ORIGINAL)** The system of claim 2, wherein the user authenticates directly with the authentication database.

4. **(ORIGINAL)** The system of claim 3, wherein the one authentication component is configured to link a user directly to the authentication database.

5. **(ORIGINAL)** The system of claim 3, wherein the one authentication component is not privy to any authentication information that passes between the user and the authentication database.

a6

6. **(ORIGINAL)** The system of claim 3, wherein authentication takes place between the user and the authentication database in a secure manner.

7. **(ORIGINAL)** The system of claim 6, wherein the authentication takes place using secure socket link (SSL) techniques.

8. **(ORIGINAL)** The system of claim 3, wherein the authentication database is configured to notify the one authentication component when a user has been properly authenticated.

9. (ORIGINAL) The system of claim 8, wherein the authentication database is configured to provide user information to the one authentication component after the user has been authenticated.

10. (ORIGINAL) The system of claim 9, wherein the user information that is provided by the authentication database comprises billing information.

11. (ORIGINAL) The system of claim 1, wherein the authentication database comprises a locally accessible authentication database.

12. (ORIGINAL) The system of claim 1, wherein the one authentication component is configured to issue a unique token to each user once the user is authenticated by the authentication database, the unique token being provided for use with data packets that can be transmitted from each user.

13. (ORIGINAL) The system of claim 1, wherein the one access module is configured to enable the user to wirelessly access the host network.

14. **(CURRENTLY AMENDED)** An authentication system for providing authentication for users who desire to access the Internet, the system comprising:

at least one host organization network configured to access the Internet, the host organization network comprising one or more subnets each of which comprising:

at least one server configured to receive data packets from individual client computing devices and transmit the data packets to the Internet; and

a plurality of public access points each of which configured to receive wireless communication from a user that is using a client computing device to wirelessly transmit data packets that are intended for the Internet and provide the wirelessly transmitted data packets to the one server before the data packets are transmitted to the Internet; and

at least one globally accessible authentication database that contains information that can be used by the database to authenticate a user without requiring the user to be affiliated with a particular Internet Service Provider (ISP).

15. **(ORIGINAL)** The system of claim 14, wherein the user authenticates directly with the globally accessible authentication database.

16. **(ORIGINAL)** The system of claim 14, wherein the one server is not privy to authentication information that is passed between the client computing device and the globally accessible authentication database.

17. **(ORIGINAL)** The system of claim 14, wherein authentication takes place between the client computing device and the globally accessible database in an end-to-end secure manner.

18. **(ORIGINAL)** The system of claim 17, wherein the secure manner comprises secure socket layer (SSL) techniques.

19. **(ORIGINAL)** The system of claim 14, wherein the globally accessible authentication database is configured to notify the one server when a user has been authenticated.

a6

20. **(ORIGINAL)** The system of claim 19, wherein the globally accessible authentication database is configured to provide user information to the one server when the user has been authenticated.

21. **(ORIGINAL)** The system of claim 20, wherein the user information that is provided to the one server by the globally accessible authentication database comprises billing information.

22. **(ORIGINAL)** The system of claim 14, wherein the user is unaffiliated with any Internet Service Providers (ISPs).

23. **(CURRENTLY AMENDED)** An authentication system for providing authentication for users who desire to access the Internet, the system comprising:

multiple wireless nodes through which the Internet can be accessed;

multiple access points with which the wireless nodes can communicate;

a server configured to receive wireless communication from the multiple access points, the server configured to enable authentication of various users; and

at least one global authentication database that contains user information that can be used to authenticate the users without requiring the users to be affiliated with a particular Internet Service Provider (ISP).

24. **(ORIGINAL)** The system of claim 23, wherein the server is configured to enable a user to log directly onto the one global authentication database.

25. **(ORIGINAL)** The system of claim 24, wherein the server is configured to present a web page having a link to the one global authentication database.

26. **(ORIGINAL)** The system of claim 24, wherein the server is not privy to any of the authentication information that gets passed between the user and the one global authentication database.

27. **(ORIGINAL)** The system of claim 24, wherein the one global authentication database is configured to notify the server after the user has been authenticated.

28. **(ORIGINAL)** The system of claim 27, wherein the one global authentication database is configured to provide user information to the server after the user has been authenticated by the global authentication database.

29. **(ORIGINAL)** The system of claim 23, wherein the server is configured to issue a unique token to the user after the user is authenticated.

a6

30. **(ORIGINAL)** The system of claim 29, wherein the server encrypts the unique token before issuing it to the user.

31. **(ORIGINAL)** The system of claim 23, wherein the multiple access points are arranged to define a wireless subnet.

32. **(ORIGINAL)** The system of claim 23, wherein the multiple access points are deployed in a publicly accessible area.

33. **(ORIGINAL)** The system of claim 23, wherein the multiple wireless nodes comprise mobile computing devices.

34. (CURRENTLY AMENDED) A method of authenticating a user for Internet access, the method comprising:

establishing a communication link between a mobile computing device and a server that is configured to provide Internet access;

contacting a global authentication database that contains user information that can be used to authenticate one or more users;

authenticating a user using the information that is contained in the global authentication database, independent of any user affiliation with any Internet Service Providers (ISPs);

notifying the server that the user has been authenticated; and

issuing a unique token to the user for use when sending data packets to the server for transmission to the Internet.

35. (ORIGINAL) The method of claim 34, wherein the communication link comprises at least one wireless link.

36. (ORIGINAL) The method of claim 34, wherein the communication link comprises a wireless link that includes the mobile computing device.

37. (ORIGINAL) The method of claim 34, wherein the communication link comprises a wireless link that includes the server.

38. (ORIGINAL) The method of claim 34, wherein the communication link comprises a wireless link that includes both the mobile computing device and the server.

39. (ORIGINAL) The method of claim 34, wherein said authenticating comprises authenticating the user using a secure protocol.

40. (ORIGINAL) The method of claim 39, wherein the server is not privy to any authentication information that passes between the user and the authentication database.

a6

41. (ORIGINAL) The method of claim 34, wherein the server comprises part of a publicly deployed and accessible host network.

42. (CURRENTLY AMENDED) One or more computer-readable media having computer-readable instructions thereon which, when executed by one or more computers, cause the computers to:

establish a wireless communication link between a mobile computing device and a server that is configured to provide Internet access;

contact a global authentication database that contains user information that can be used to authenticate one or more users;

authenticate a user using the information that is contained in the global authentication database, independent of requiring the user to be affiliated with a particular Internet Service Provider (ISP);

notify the server that the user has been authenticated; and

issue a unique token to the user for use when sending data packets to the server for transmission to the Internet.

43. (CURRENTLY AMENDED) A method of authenticating a user for Internet access, the method comprising:

configuring multiple access points to receive wireless communication from multiple wireless nodes through which the Internet can be accessed, the multiple wireless nodes being capable of communicating data packets that are intended for transmission to the Internet;

configuring a server to wirelessly receive the data packets that are communicated to the multiple access points; and

configuring a globally accessible database that includes information that can be used to authenticate one or more users that desire to access the Internet, authentication taking place in a manner that does not require the one or more users to be affiliated with a particular Internet Service Provider (ISP).

44. (ORIGINAL) The method of claim 43 further comprising using the globally accessible database to authenticate one or more users.

45. (ORIGINAL) The method of claim 44, wherein said using comprises linking the user directly to the globally accessible database.

46. **(ORIGINAL)** The method of claim 44, wherein said using comprises linking the user directly to the globally accessible database and authenticating the user outside of the purview of the server.

47. **(ORIGINAL)** The method of claim 44, wherein said using comprises linking the user directly to the globally accessible database and notifying the server when the user has been authenticated.

Q6

48. **(ORIGINAL)** The method of claim 44 further comprising issuing a user, once authenticated, a unique token that uniquely identifies that user.

49. **(ORIGINAL)** The method of claim 43, wherein at least some of the wireless nodes comprise mobile computing devices.